Sharemind-privaatsust säilitav analüüs

Baldur Kubo

baldur.kubo@cyber.ee

CYBERNETICA

sharemind

PRIST

Eestis Sharemindiga läbi viidud uuring PRIST
privaatsust-säilitavad statistilised uuringud ühendatud andmebaasides
Esimene krüptograafiliselt privaatne registripõhine uuring maailmas.

Finantseeris SA Archimedes Euroopa Regionaalarengufondi „Info- ja kommunikatsioonitehnoloogia alase teadus- ja arendustegevuse toetamise“ alameetmest

Toetas Euroopa Liidu 7. raamprogrammi teadusprojekt Usable and Efficient Secure Multi-party Computation (UaESMC)

sharemind

Mis on Sharemind?

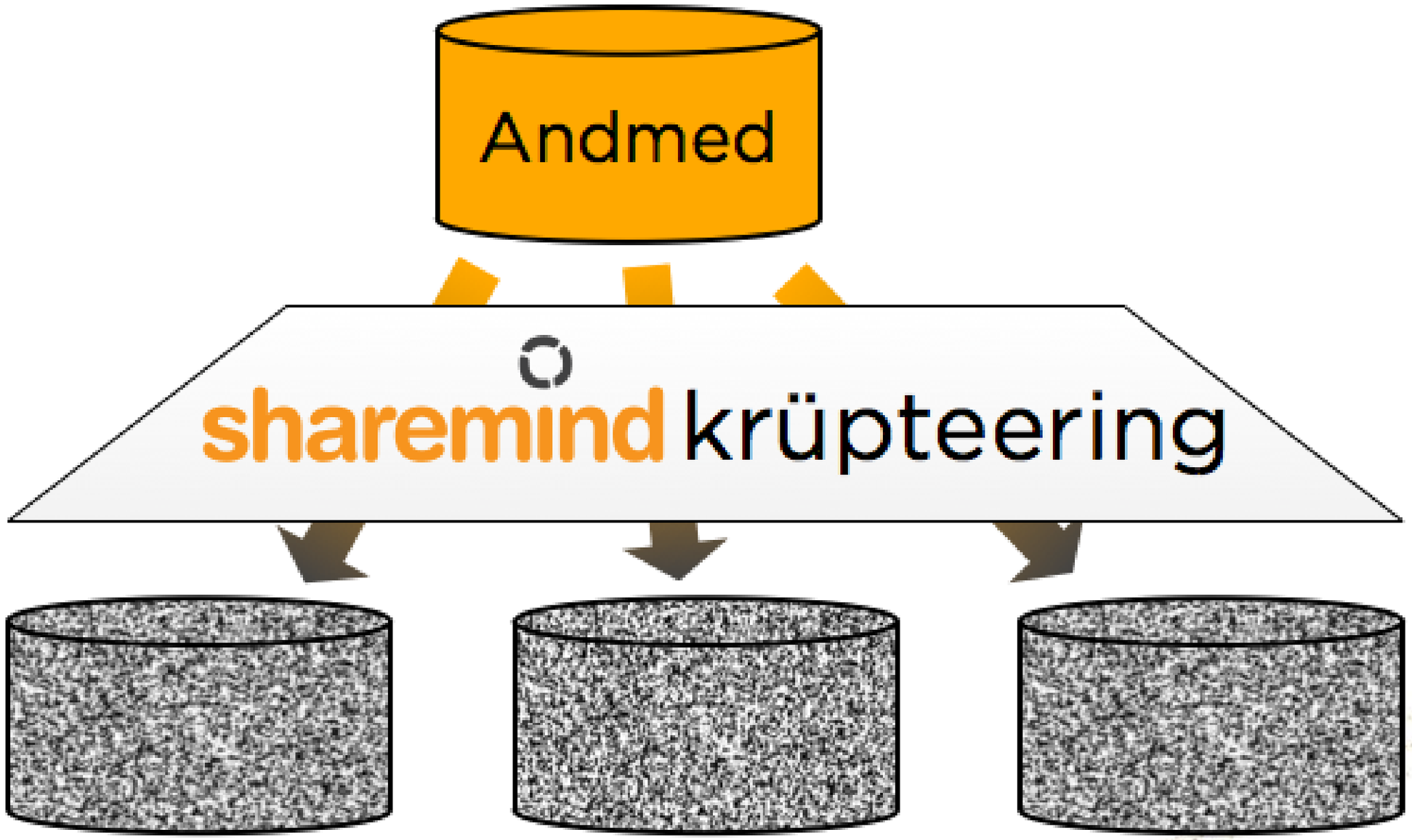
Sharemind on tööriist isikuandmete ja ärisaladuste krüptograafiliselt turvaliseks analüüsimiseks.

Sharemindi on alates 2007. aastast arendanud Cybernetica AS teadurite ja inseneride meeskond.

Sharemind pakub tõestatavat kaitset privaatsete andmete lekkimise eest analüüsi käigus.

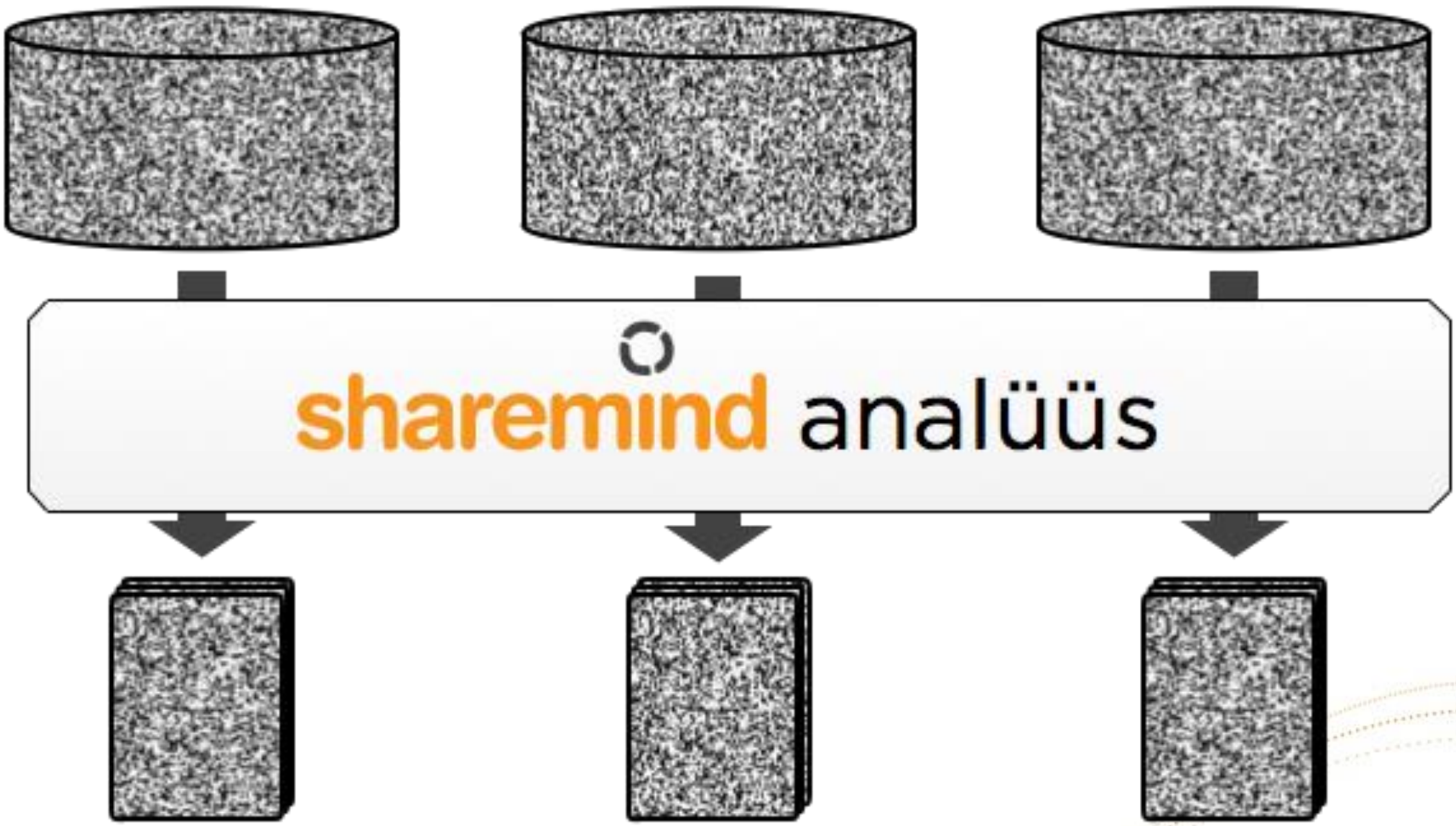
sharemind

Omanik kaitseb andmeid



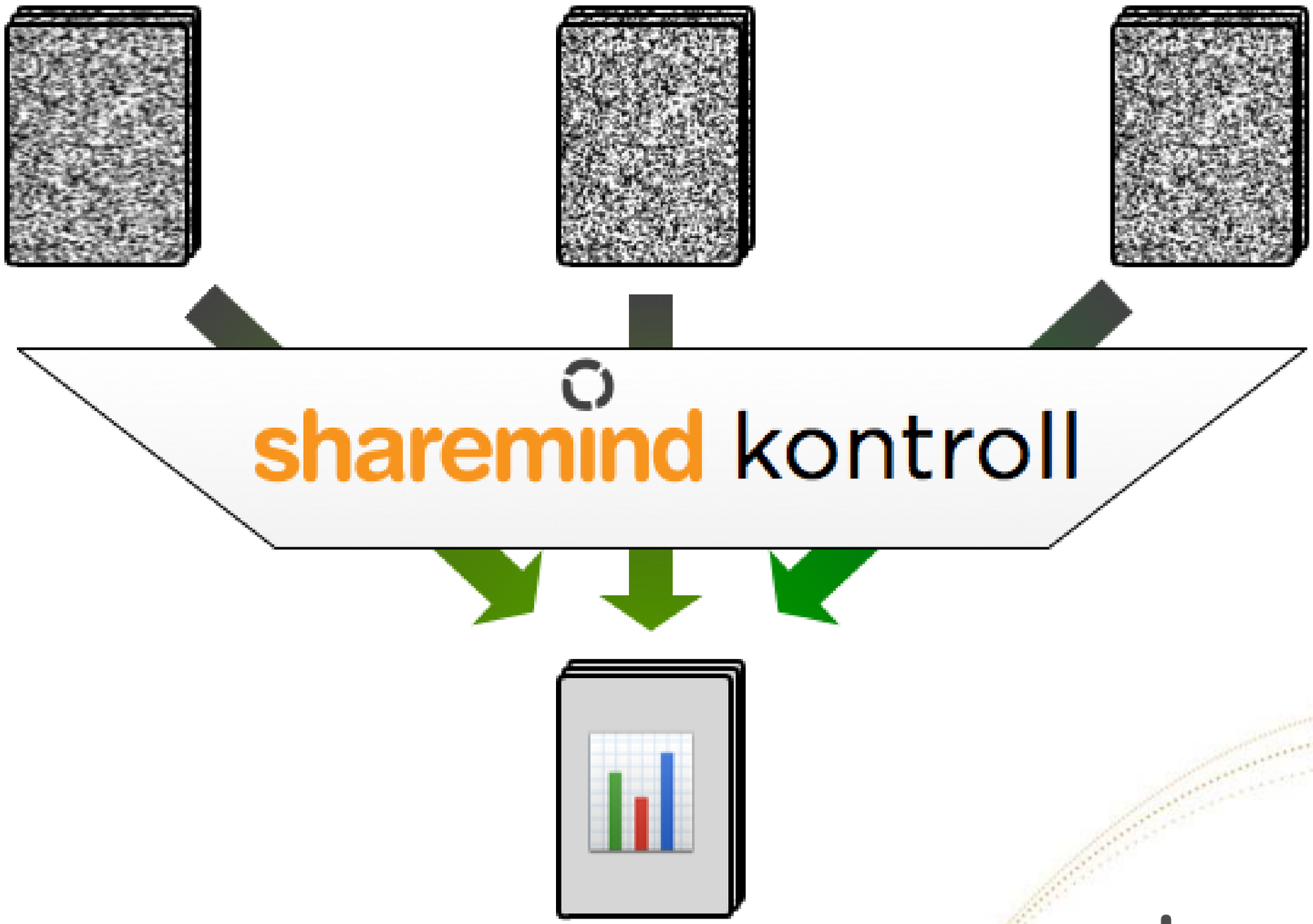
sharemind

Sharemind andmeid ei näe



sharemind

Analüütik näeb tulemeid



sharemind

Tehniline lahendus (1)

Sharemind kogub ja salvestab andmeid *krüptograafilise ühissalastuse* abil.

Ühissalastus teeb salajased väärtused matemaatiliselt juhuslikeks osadeks ning jagab osad sõltumatute serverite vahel.

Ükski server ei suuda enda osa põhjal saladust taastada.

sharemind

Tehniline lahendus (2)

Sharemind töötleb andmeid *krüptograafiliselt turvalise ühisarvutuse* abil.

Turvaline ühisarvutus lubab mitmel serveril teha arvutusi ühissalastatud andmetel ilma, et saladusi osadest tagasi kokku pandaks.

Ükski server ei näe arvutuste käigus salajasi andmeid.

sharemind

Isik A

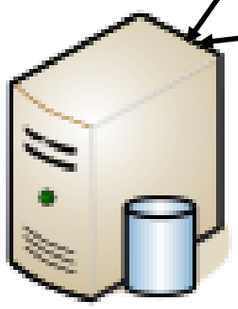
Vanus: 25

Isik B

Vanus: 33

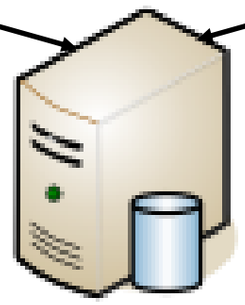
1. Vali juhuslik arv $a_1 = 57$
2. Vali juhuslik arv $a_2 = 13$
3. Arvuta $a_3 = 25 - 57 - 13 \equiv 55 \bmod 100$
4. Saada iga a_k eraldi serverile

1. Vali juhuslik arv $b_1 = 44$
2. Vali juhuslik arv $b_2 = 57$
3. Arvuta $b_3 = 33 - 44 - 57 \equiv 32 \bmod 100$
4. Saada iga b_k eraldi serverile



Server 1

$a_1 = 57$
$b_1 = 44$
$c_1 = a_1 + b_1 = 101$
$\equiv 1 \bmod 100$



Server 2

$a_2 = 13$
$b_2 = 57$
$c_2 = a_2 + b_2 = 70$
$\equiv 70 \bmod 100$

Server 3

$a_3 = 55$
$b_2 = 32$
$c_3 = a_3 + b_3 = 87$
$\equiv 87 \bmod 100$

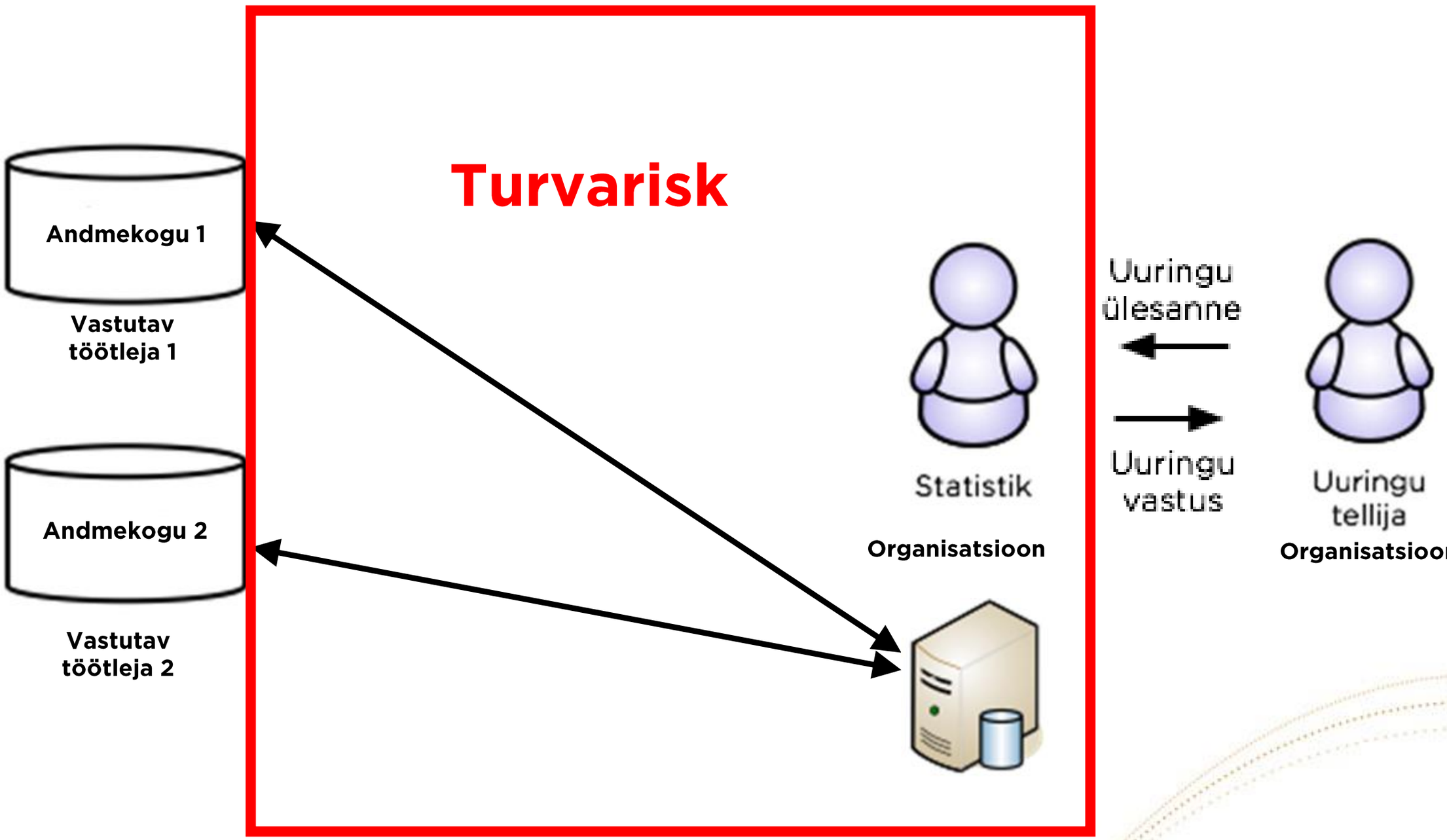
Isik C

C arvutab $c = 1 + 70 + 87 = 158 \equiv 58 \bmod 100$

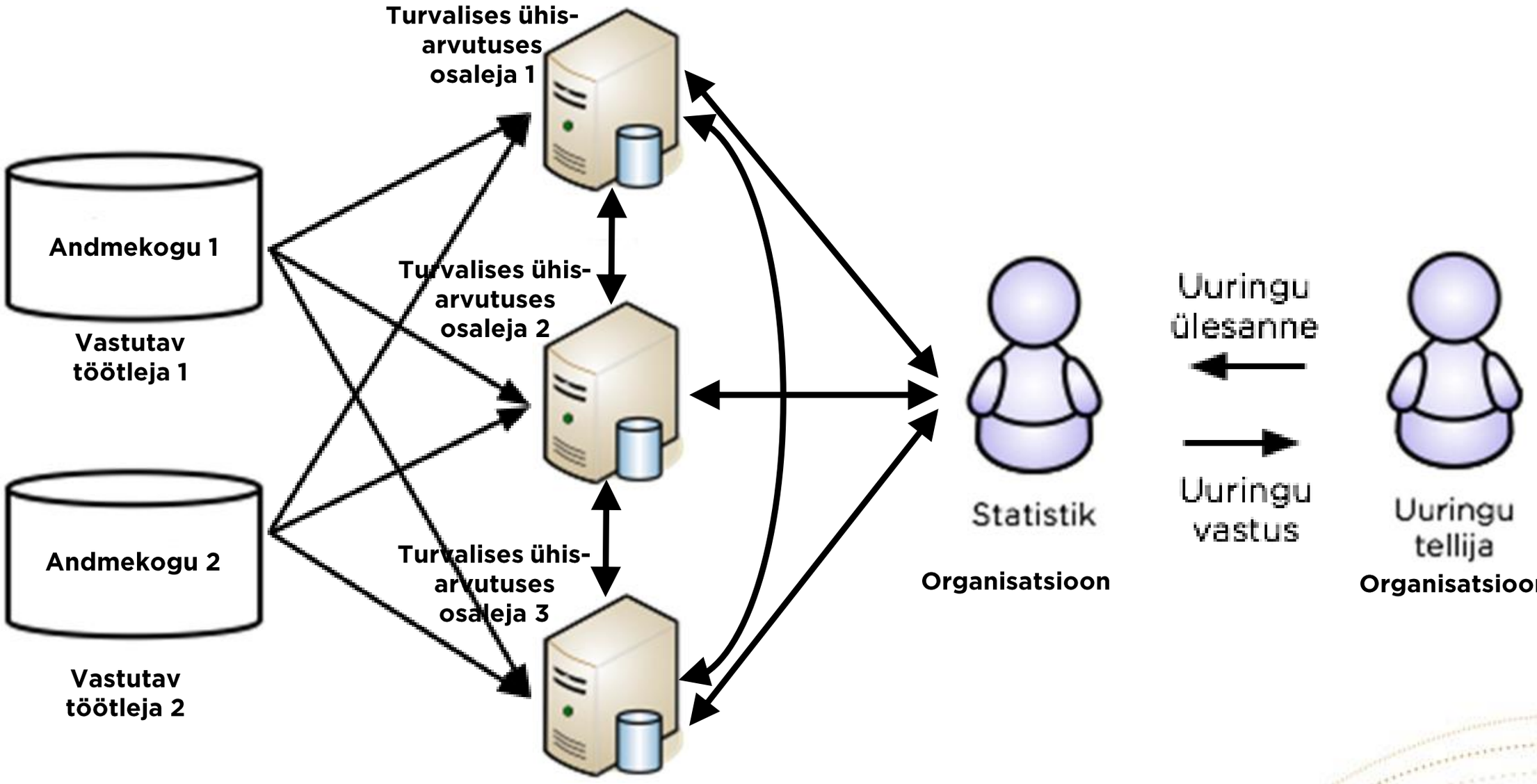
C sai teada, et A ja B vanuste summa on 58
Ei C ega serverid ei näinud A ja B vanuseid

sharemind

Tavapärane uuringu protsess

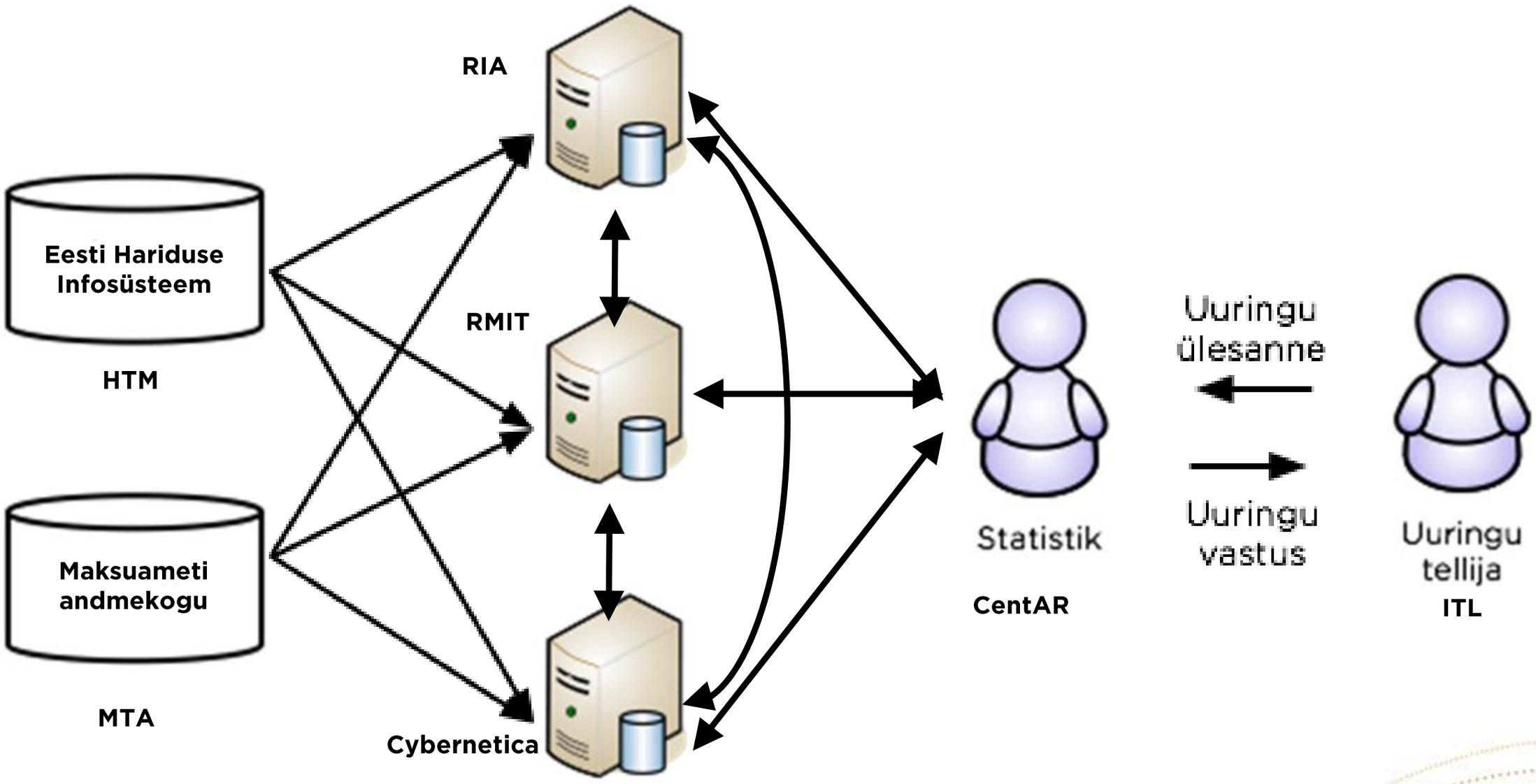


Sharemindi uuringu protsess



andmeomanikul (vastutav töötleja)
võimalik pöörata oma luba andmeid kasutada

Privaatsust säilitav statistika



PRIST
privaatsust-säilitavad statistilised uuringud ühendatud andmebaasides

sharemind

AKI hinnang Sharemindile

“Teie esitatud taotlusest ja lisadokumentidest selgub, et teadusuuringu raames isikuandmete ja delikaatsete isikuandmete töötlemist Teie poolt ei toimu. Andmesubjektid muudetakse tuvastamatuks kasutades ühissalastust ning Teie töötlete tuvastamatuks muudetud (krüpteeritud) andmeid. “

AKI, 27.01.2014 dokumendi nr 2.2.-7/13/557r

sharemind

Sharemind võimaldab

Turvaliselt jagada informatsiooni:

Avaliku ja erasektori vahel (registripõhised uuringud, elutähtsate teenuste analüüs, terviseandmete analüüs, maksupettuste analüüs)

Koostööpartnerite vahel (meditsiiniuuringud, olukorra ülevaated, riskihinnangud, võrdlusanalüüs, oksjonid, tarneahela analüüs)

Organisatsioonis (töötajarahulolu jm uuringud)

sharemind

sharemind

https://sharemind.cyber.ee/

sharemind@cyber.ee